対称3進巡回AN符号 (多値論理およびその応用)

AUTHOR(S):

大倉, 良昭; 島田, 良作; 長谷川, 利治

CITATION:

大倉, 良昭 ...[et al]. 対称3進巡回AN符号 (多値論理およびその応用). 数理解析研究所講究録 1982, 455: 231-244

ISSUE DATE:

1982-03

URL:

http://hdl.handle.net/2433/103015

数理解析研究所講究録
455巻 1982年 231-244

対称3進巡回AN符号

徳島文理大　　大倉 良昭
徳大 工学部　　島田 良作
京大 工学部　　長谷川利治

1. はじめに　算術AN符号[1]は算術演算装置および伝送路よりなるディジタルシステムの高信頼化を目的とした誤り検出訂正符号である。D.T. Mandelbaum[2]はハミング距離に基づく代数的巡回符号に類似な性質をもつ算術AN符号を発見した。巡回AN符号と呼ばれるこの符号はN. Tsao-Wu[3]をはじめ多くの研究者により相当の成果が得られている[4][5]。以上は主に2進符号に関するものであるが，これらを拡張した非2進符号についてもいくつかの研究がある[6][7]。本報告では3進独特の巡回AN符号が提案される。

算術AN符号とは整数Nに一定数Aを乗算したものANの集合である。3進算術AN符号では元ANの3進表現を符号語とする。Aは生成数と呼ばれ，これは3と互いに素$((A,3)=1)$な正整数に選ばれる。符号語AN_1とAN_2の加減算結果は$A(N_1 \pm N_2)$となり，やはり整数$(N_1 \pm N_2)$のA倍である。符号長nの3進算

術AN符号の任意の符号語ANは

$$AN=(a_{n-1}\ a_{n-2}\cdots a_0)_3 \qquad (1)$$

であり，これを1けた左巡回けた移動したものは

$$(a_{n-2}\cdots a_0\ a_{n-1})_3 = AN3-a_{n-1}(3^n-1) \qquad (2)$$

と書ける。式(2)がやはり同じ符号の符号語であるための必要十分条件は，$3^n-1=AB$ を満たす整数Bが存在することである。ここで，$(A,3)=1$ であるから，$(B,3)=1$ である。又，Bは符号語数を意味する。法Bに関して3が属するべき数$E(3,B)$をe_1とすれば，

$$3^{e_1}-1\equiv 0 \pmod{B} \qquad (3)$$

が成立する。従って，符号語数Bを与えて符号長$n(=e_1)$，生成数$A(=(3^{e_1}-1)/B)$の算術AN符号が構成できる。しかもこの符号は巡回けた移動のもとに閉じている。このような巡回AN符号は法3^n-1に関する完全剰余系におけるAの倍数すべての集合である。

式(1)で示される符号語に対称3進表現(ST表現)を用いるST-AN符号[8]がある。ここで述べる3進巡回AN符号は法3^n-1に関する絶対最小完全剰余系[9]において定義されるST-AN符号である。ST算術重み[8]に基づく算術距離が整数の有限な環上で定義される。これは，従来の算術重み[1]を同様な環上で定義したモジュラ重み，モジュラ距離[10]に対応しており，実際的

である。次に，符号の誤り検出訂正能力の評価方法を述べる。さらに，符号語数Bが特別な条件を満たすとき，この符号の最小距離を与える公式を導く。

2. 巡回ST-AN符号　ST-AN符号の符号語$A\alpha$は

$$A\alpha=(a_{n-1}\ a_{n-2}\cdots a_0)_{ST},\ (a_i\in\{\bar{1},0,1\},\ i=0,1,\cdots,n-1) \quad (4)$$

で表され，$(A,3)=1$である。

〔定義1〕　ST-AN符号が巡回けた移動のもとに閉じているとき，この符号を巡回ST-AN符号という。

1章で述べたように，3と互いに素な整数Bに対して，符号長nおよび生成数Aを

$$n=e_1,\quad A=(3^{e_1}-B)/B \qquad (5)$$

とするST-AN符号は巡回けた移動のもとに閉じており，巡回ST-AN符号である。以下，この符号語数Bによって構成される巡回ST-AN符号II_Aを考える。

法$3^n-1\ (=AB)$に関する絶対最小完全剰余系R_{AB}を

$$R_{AB}=\left\{1-\frac{3^n-1}{2},\ 2-\frac{3^n-1}{2},\ \cdots,\ -1,\ 0,\ 1,\ \cdots\right.$$
$$\left.\cdots,\ \frac{3^n-1}{2}-1,\ \frac{3^n-1}{2}\right\} \qquad (6)$$

とする。R_{AB}は法3^n-1に関する加算と乗算のもとに環をなす。II_Aは環R_{AB}において正整数Aで生成されるイデアルである。又，法Bに関する絶対最小完全剰余系R_Bを

$$R_B=\left\{-\frac{B-1}{2},\ 1-\frac{B-1}{2},\ \cdots,\ -1,\ 0,\ 1,\ \cdots,\ \frac{B-1}{2}-1,\ \frac{B-1}{2}\right\},\ (B:\text{奇数}) \quad (7)$$

$$R_B=\{1-\frac{B}{2},\ 2-\frac{B}{2},\ \cdots,\ -1,\ 0,\ 1,\ \cdots,\ \frac{B}{2}-1,\ \frac{B}{2}\},\ (B:\text{偶数})$$

とする。このとき，I_A は R_B の元の A 倍すべての集合であり，

$$I_A = A\cdot R_B \tag{8}$$

と書く。

3. モジュラST距離と符号の最小距離　ST算術重み W_{ST} は任意の整数 N のST表現 $(a_{n-1}\ a_{n-2}\cdots a_0)_{ST}$ により，

$$W_{ST}(N)=\sum_{i=0}^{n-1}|a_i| \tag{9}$$

である。以下，このST算術重みを簡単にST重みという。

〔定義2〕　2整数 N_1，N_2 の間のモジュラST距離(MST距離)を

$$D_{MST}(N_1,\ N_2)=W_{ST}((N_1-N_2)\bmod(3^n-1)) \tag{10}$$

とする。ここで，$(N_1-N_2)\bmod(3^n-1)$ は，N_1-N_2 の法 3^n-1 に関する絶対最小剰余であり，環 R_{AB} の元である。

このMST距離がメトリック関数であること，すなわち距離に関する三公理，

$$\left.\begin{aligned} &D_{MST}(N_1,N_2)\geqq 0\\ &D_{MST}(N_1,N_2)=D_{MST}(N_2,N_1)\\ &D_{MST}(N_1,N_2)\leqq D_{MST}(N_1,N_3)+D_{MST}(N_3,N_1)\end{aligned}\right\} \tag{11}$$

を満たすことはST重みの基本的性質[8]を用いて証明される。

巡回ST-AN符号 I_A がイデアルであって，

$$(A\alpha_1\pm A\alpha_2)\bmod(AB)=A[(\alpha_1\pm\alpha_2)\bmod B] \tag{12}$$

であるから，$(A\alpha_1 \pm A\alpha_2) \bmod (AB)$ も符号語である。すなわち，巡回ST-AN符号 $\mathbb{I}_A$ は線形な符号である。このため，任意の符号語 $A\alpha_1$ と $A\alpha_2$ の間のMST距離に等しいST重みをもつ第三の符号語 $A\alpha_3$ が存在し，$\mathbb{I}_A$ の最小MST距離 d_m と最小ST重みは等しい。

雑音や装置の障害のため符号語に加えられるれけた以下のST数でそのST重みが d であるものを d 重の算術誤りという。このとき，次の定理と系が成立する。

〔定理1〕 巡回ST-AN符号 $\mathbb{I}_A$ の最小MST距離 d_m が $d+1(2t+1)$ に等しいとき，そのときに限って，$d(t)$ 重以下のすべての算術誤りの検出（訂正）が可能である。

〔系1.1〕 巡回ST-AN符号 $\mathbb{I}_A$ の最小MST距離 d_m が $t+d+1, (t<d)$ のとき，そのときに限って，t 重以下の算術誤りの訂正と d 重以下の算術誤りの検出が可能である。

4. 最小距離の評価 巡回ST-AN符号 $\mathbb{I}_A$（式(8)）は B の約数 d_i $(1 \leqq d_i \leqq B)$ により，

$$\mathbb{I}_A = A \sum_{d_i | B} d_i \cdot G(B/d_i) \qquad (13)$$

と表すことができる。ここで，$G(B/d_i)$ は法 B/d_i に関する絶対最小既約剰余系である。ただし，$d_i = B$ のとき，$G(1)$ は $\{0\}$ を意味する。式(13)の各項 $Ad_i \cdot G(B/d_i)$ を部分符号という。各部分符号には $\mathbb{I}_A$ の符号語が $G(B/d_i)$ の位数 $\varphi(B/d_i)$ 個だけ含ま

れる。ここに，φはオイラ関数である。さらに，$G(B/d_i)$は巡回部分群

$$\mathbb{H}^{(1)}(B/d_i)=\{3^k \bmod (B/d_i) \mid k=1,2,\cdots e_i\},\ (e_i=E(3,B/d_i)$$

により，$\nu_i=\varphi(B/d_i)/e_i$ 個のコセット

$$\mathbb{H}^{(j)}(B/d_i)=\{b_j 3^k \bmod (B/d_i) \mid k=1,2,\cdots,e_i\},$$

$$(^\exists b_j \in G(B/d_i)) \qquad (14)$$

に展開できる。各コセットのすべての元(e_i個)のAd_i倍の集合を素符号という。この素符号に含まれる符号語はその任意の符号語を巡回けた移動したもので尽されている(強巡回的)。従って，素符号に含まれる符号語のST重みはすべて相等しい。このST重みを素符号のST重みという。

巡回ST-AN符号$\mathbb{I}_A$の任意の符号語$A\alpha$の各けたα_ℓの値は，

$$\alpha_\ell=-(B \bmod 3)[(\alpha 3^{n-\ell} \bmod B) \bmod 3],\ (\ell=0,1,\cdots n-1) \quad (15)$$

で与えられる[6]。$(B,3)=1$であるから，$B \bmod 3=1$または-1である。従って，α_ℓが零か非零かは，$\alpha 3^{n-\ell} \bmod B$が3の倍数か否かによる。素符号$Ad_i \cdot \mathbb{H}^{(j)}(B/d_i)$のひとつの符号語$A\alpha=Ad_ib_j$について，そのST重みを考える。式(15)について，

$$d_i b_j 3^{n-\ell} \bmod B = d_i(b_j 3^{n-\ell} \bmod (B/d_i))$$

であり，$(d_i,3)=1$。ℓが0から$n-1$までを変るとき，$3^{n-\ell}$は3^1から3^nを変る。このとき，$b_j 3^{n-\ell} \bmod (B/d_i)$は$\mathbb{H}^{(j)}(B/d_i)$の元を丁度$n/e_i(=e_1/e_i)$通り変る。以上により，次の定理

を得る。

〔定理2〕 素符号 $Ad_i \cdot \mathcal{H}^{(i)}(B/d_i)$ のST重みは，$\mathcal{H}^{(i)}(B/d_i)$ の元のうち3の倍数でないものの個数の e_1/e_i 倍に一致する。ここで，$e_1 = E(3, B)$，$e_i = E(3, B/d_i)$ である。

巡回ST-AN符号 $\mathbb{A}_A$ の最小MST距離は $\mathbb{A}_A$ を構成する $\{0\}$ を除く素符号のST重みの最小値であり，素符号のST重みは絶対最小完全剰余系 R_B の分解により定理2で評価できる。

5. 簡単な構造をもつ巡回ST-AN符号 $\mathbb{A}_A$ の最小距離 符号語数 B が特別な条件を満たすとき，その条件の範囲で一般的に $\mathbb{A}_A$ の最小MST距離 d_m を与える公式を導くことができる。以下では，B が5以上の素数 P により，$B = P$，$2P$，$4P$ で表される場合について例示する。

5.1 $B = P$ で規定される符号 P は素数であるから，B の約数は1と P 自身である。この場合の巡回ST-AN符号 $\mathbb{A}_A$ は，

$$\mathbb{A}_A = A \cdot G(P) + A \cdot G(1), \quad (G(1) = \{0\}) \tag{17}$$

のように2個の部分符号に分解される。ここで，$\{0\}$ は符号語 $(00\cdots0)_{ST}$ である。以下，法 P に関して3が原始根である場合と3でなく -3 が原始根である場合を考える。

(a) 法 P に関して3が原始根の場合 法 P に関して3が属するべき数 $e_1 = \varphi(P) = P - 1$ である。この符号の符号長 n と生成数 A は式(5)により，

$$n=e_1=P-1,\quad A=(3^n-1)/P \tag{18}$$

で与えられる。法Pに関して3が原始根であるから，法Pに関する絶対最小既約剰余系$G(P)$は，

$$G(P)=\{3^k \bmod P \mid k=1,2,\cdots,P-1\}.$$

従って，式(17)の$A\cdot G(P)$は強巡回的な素符号である。

$$G(P)=H^{(1)}(P)=\{\pm g \mid g=1,2,\cdots,(P-1)/2\}$$

であるから，定理2により，最小MST距離d_mは，

$$d_m=\begin{cases}\frac{2}{3}(P-1), & (P\equiv 1 \pmod 3)\\ \frac{2}{3}(P+1), & (P\equiv -1 \pmod 3)\end{cases} \tag{19}$$

(b) 法Pに関して3でなく-3が原始根の場合

〔定理3〕 $(m,3)=1$なる正整数mにおいて，法mに関して3でなく-3が原始根のとき，そのときに限って，

$$E(3,m)=\varphi(m)/2,\quad (\text{奇数}) \tag{20}$$

定理3により，$E(3,P)=e_1=(P-1)/2$である。符号長と生成数は

$$n=(P-1)/2,\quad A=(3^n-1)/P \tag{21}$$

である。部分符号$A\cdot G(P)$は2個の素符号に分解される。すなわち，$G(P)$は2個のコセット$H^{(1)}(P)$と$H^{(2)}(P)$に展開され，$G(P)$の元1は$H^{(1)}(P)$に含まれ，-1は$H^{(2)}(P)$に含まれる。このことは$E(3,P)$が奇数であることによる。$H^{(2)}(P)\equiv -1\cdot H^{(1)}(P)$となり，両素符号のST重みは等しく，(a)の場合の$H^{(1)}(P)$を参

考にすることができる。ところが，次の定理が成立する。

〔定理4〕　$P\equiv 1 \pmod 3$, $P\geq 5$ なる素数 P に対して，-3 は法 P に関する原始根であり得ない。

この定理は原始根と平方剰余，平方非剰余[9]の関連により導かれる。この符号の最小MST距離 d_m は，式(19)第二式に対応して得られ，

$$d_m = \frac{1}{3}(P+1) \tag{22}$$

以上の(a),(b)で述べた符号は等距離符号である。

5.2　$B=2P$ で規定される符号

$B=2P$ の約数 1, 2, P, 2P により，このようなBで規定される巡回ST-AN符号は

$$\mathbb{I}_A = A\cdot G(2P) + A2\cdot G(P) + AP\cdot G(2) + Ap2\cdot G(1),$$

$$(G(1)=\{0\},\ G(2)=\{1\}) \tag{23}$$

〔定理5〕　法 P に関して3(−3)が原始根であるとき，3(−3)は法 $2P$ に関して原始根である。

(α) 法 P に関して3が原始根である場合　定理5により，

$$n = P-1,\quad A=(3^n-1)/2P. \tag{24}$$

初めに，部分符号 $Ap\cdot G(2)=\{Ap\}$ は1個の符号語 $Ap=(3^n-1)/2 = (11\cdots1)_{ST}$ からなり，

$$W_{ST}(Ap) = P-1. \tag{25}$$

次に，部分符号 $Ap\cdot G(P)$ は5.1(α)と同様にして，

$$W_{ST}(A2)=\begin{cases}\frac{2}{3}(P-1), & (P\equiv 1 \pmod 3)\\ \frac{2}{3}(P+1), & (P\equiv -1 \pmod 3)\end{cases} \qquad (26)$$

最後に，部分符号 $A\cdot G(2P)$ は，定理5により素符号であり，

$$G(2P)=\mathbb{H}^{(1)}(2P)=\{3^k \bmod 2P \mid k=1,2,\cdots,P-1\}$$

である。それゆえ，素符号のST重み $W_{ST}(A)$ は集合

$$G'(2P)=\{\pm g \bmod 3 \mid g=1,3,5,\cdots,P-2\}$$

の非零元の個数に等しい。ここで，集合

$$S_1=\{\pm g \bmod 3 \mid g=1,2,3,\cdots P-1\},$$

$$S_2=\{\pm 2g' \bmod 3 \mid g'=1,2,\cdots,(P-1)/2\}$$

の非零元の個数をそれぞれ W_1, W_2 とすれば，$W_{ST}(A)=W_1-W_2$ により与えられる。すなわち，

$$W_{ST}(A)=\begin{cases}\frac{2}{3}(P-1), & (P\equiv 1 \pmod 3)\\ \frac{2}{3}(P-2), & (P\equiv -1 \pmod 3)\end{cases} \qquad (27)$$

以上により，式(25)～(27)の最小値すなわち最小MST距離 d_m は

$$d_m=\begin{cases}\frac{2}{3}(P-1), & (P\equiv 1 \pmod 3)\\ \frac{2}{3}(P-2), & (P\equiv -1 \pmod 3)\end{cases} \qquad (28)$$

(b) 法Pに関して3でなく-3が原始根である場合 $\mathbb{I}_A$ は

$$n=(P-1)/2,\quad A=(3^n-1)/2P. \qquad (29)$$

(a)と同様にして，

$$W_{ST}(AP)=(P-1)/2. \qquad (30)$$

又，$A2\cdot G(P)$については，5.1(b)の$A\cdot G(P)$と同様であり，

$$W_{ST}(A2)=\frac{1}{3}(P+1). \tag{31}$$

最後に，部分符号$A\cdot G(2P)$は，定理5と式(27)の第二式で用いられた手法を応用して

$$W_{ST}(A)=\frac{1}{3}(P-2). \tag{32}$$

式(30)～(32)により，最小MST距離d_mは

$$d_m=\frac{1}{3}(P-2). \tag{33}$$

5.3　B=4Pで規定される符号　法B=4Pに関する既約剰余系$G(4P)$の位数は

$$\varphi(4P)=2(P-1). \tag{34}$$

B=4Pで規定される符号II_Aは，

$$\mathrm{II}_A=A\cdot G(4P)+A2\cdot G(2P)+A4\cdot G(P)$$
$$+AP\cdot G(4)+A2P\cdot G(2)+A4P\cdot G(1),\ (G(4)=\{\pm1\}) \tag{35}$$

で表され，6個の部分符号に分解される。

(a) 法Pに関して3が原始根であって，4がP-1を整除する場合　法Pに関して3が原始根であって，$E(3,P)=P-1$が偶数である。又，$E(3,4)=2$であるから，$E(3,4P)$は，

$$E(3,4P)=LCM\{E(3,4),E(3,P)\}=P-1\ (=\varphi(4P)/2).$$

このような符号II_Aは

$$n=P-1,\quad A=(3^n-1)/4P. \tag{36}$$

4がP-1を整除するから，$(P-1)/2$は偶数である。従って，

この場合，-3もまた法Pに関して原始根であり，定理4により，$P\equiv 1 \pmod 3$の場合を考える。このとき，部分符号$A4\cdot G(P)$，$A2\cdot G(2P)$は5.1，5.2の(a)と同様である。$G(4P)$に対応する部分符号，$A\cdot G(4P)$を考える。Pの与えられた条件を満たすとき，$(P-1)$未満の正整数gに対して，$3^g \equiv -1 \pmod{4P}$である。従って，$A\cdot G(4P)$は2個の素符号$A\cdot H^{(1)}(4P)$と$-A\cdot H^{(1)}(4P)$に分解され，両者の符号語のST重みは相等しい。その結果，

$$G'(4P)=\{\pm 3^k \bmod 4P \bmod 3 \mid k=1,2,\cdots,P-1\}$$

の非零元の個数の$1/2$が両素符号のST重みとなる。すなわち，

$$W_{ST}(A)=\frac{2}{3}(P-2). \tag{37}$$

なお，部分符号$A2P\cdot G(2)$，$AP\cdot G(4)$については，

$$W_{ST}(A2P)=W_{ST}(AP)=P-1. \tag{38}$$

式(37)，(38)さらに式(19)の第1式，式(28)の第1式を考慮して，

$$d_m=\frac{2}{3}(P-2). \tag{39}$$

(b) 法Pに関して3でなく-3が原始根である場合　このとき，

$$E(3,4P)=LCM\{E(3,4),E(3,P)\}=P-1=e_1$$

であり，$E(3,P)=E(3,2P)=(P-1)/2$。このような符号II_Aは

$$n=P-1,\quad A=(3^n-1)/4P. \tag{40}$$

部分符号$A\cdot G(4P)$を考える。与えられたPの条件を満たすとき，

$3^g \equiv -1 \pmod{4P}$, $(0<g<P-1)$

が成立し，$G(4P)$ は $H^{(1)}(4P)$ と $-H^{(1)}(4P)$ に分解される。両素符号のST重みは相等しく，5.3 の式(37)と同様の結果を得る。他の部分符号については5.1，5.2 の結果を応用することができ，この場合の Π_A の最小距離は式(39)に一致する。

6. おわりに　符号語数 B で規定される巡回ST-AN符号の構成とその符号の最小MST距離の算定方法を示した。又，P が特別な条件を満たす場合の $B=P$, $2P$, $4P$ で規定される符号の最小MST距離を与える公式を得た。生成数 A を与えてその符号語を定めるST-AN符号[8]では，最小距離 d が4以下の場合を除けば，組織的な構成方法が得られていない。巡回ST-AN符号の場合，多重誤り検出訂正符号も比較的能率よく構成できる。5章で述べた巡回ST-AN符号の生成数 $A=(3^n-1)/B$ は，P が大きくなるに従って，著しく大きくなり，符号能率は大きく低下する。最小距離 $d=3,4$ のST-AN符号の例[8]の一部は巡回ST-AN符号であり，5章の B を生成数にもつ双対的な符号である。なお，復号法の研究が残されている。

文献 (1) Peterson, W. W and Weldon, Jr. E.J.: "Error Correcting Codes", 2nd ed. M.I.T. Press, Cambridge, Mass. (1972)
(2) Mandelbaum, D.: "Arithmetic codes with large distance", IEEE Trans. Inform. Theory, Vol. IT13, PP. 237-242. (1967)

(3) Tsao-Wu, N.: "Arithmetic cyclic codes", Northeastern Univ., Boston, Mass., Part I of Communication Theory Group Report, No-10. (1968)

(4) Chien, R.T., Hong, S.J. and Preparata, F.P.: "Some results in theory of arithmetic codes", Coordinate Science Labs., Univ. of Illinois, Urbana, Report, R-440. (1969)

(5) Hartman, W.F.: "A note on arithmetic codes and arithmetic distance", Technical Report EE-705, Univ. of Notre Dame. (1970)

(6) 福村, 後藤: "算術符号理論", 電気電子工学大系40, コロナ社. (昭和53)

(7) Ecker, A.: "How to compute the minimum distance for cyclic AN-code over an arbitrary base", Inf. and Cont., 46, PP219-240. (1980)

(8) 大倉, 島田, 長谷川: "対称3進算術AN符号", 信学論(D), J64-D, 6, PP. 502-509. (昭56-06)

(9) ヴィノグラードフ著三瓶, 山中訳: "整数論入門", 共立出版. (昭34-11)

(10) Rao, T.R.N. and Garcia O.N.: "Cyclic and multiresidue codes for arithmetic operation", IEEE Trans. Inf. Theory, IT-17, PP85-91. (1971)